ONE DIMENSIONAL CONVOLUTIONAL GOPPA CODES OVER THE PROJECTIVE LINE

J.A. DOMÍNGUEZ PÉREZ, J.M. MUÑOZ PORRAS AND G. SERRANO SOTELO

Abstract. We give a general method to construct MDS one-dimensional convolutional codes. Our method generalizes previous constructions [5]. Moreover we give a classification of one-dimensional Convolutional Goppa Codes and propose a characterization of MDS codes of this type.

Introduction

One of the main problems in coding theory is the construction of codes with a large distance, such as so-called MDS codes.

The aim of this paper is to give a very general method to construct one-dimensional MDS convolutional codes using the techniques developed in our previous papers [1, 2, 3].

In Section 1 we give a general introduction to convolutional codes, reformulated in terms that enables a good understanding of the choices of the generator matrices and the submodules generated by them. The treatment is fairly self-contained, with only a few references for proofs of certain statements. Moreover, a characterization of one-dimensional MDS convolutional codes in terms of their associated block linear codes is given (Theorem 1.11).

In Section 2 we describe the notion of Convolutional Goppa Code, introduced in [1] and [2] and we recall the construction of convolutional Goppa codes over the projective line. We use this construction in Section 3 to give families of examples of one-dimensional convolutional Goppa codes; moreover, we prove, using Theorem 1.11, that they are MDS. This is the main result in this paper. The examples constructed in [5] are particular cases of ours.

Finally, we give in Section 3.1 a classification of one-dimensional convolutional Goppa codes defined over the projective line, which could give rise to a characterization of MDS convolutional Goppa codes of dimension one.

1. Convolutional codes

Given a finite field $\mathbb{F}_q$, representing the symbols in which an information word $u \in \mathbb{F}_q^k$ is written, each $k \times n$ matrix of rank k with entries in $\mathbb{F}_q$ defines an injective linear map

$$\begin{aligned} \mathbb{F}_q^k &\xrightarrow{\mathcal{G}} \mathbb{F}_q^n \\ u &\mapsto x = u\mathcal{G}\,, \end{aligned}$$

This work was partially supported by the research contracts MTM2009-11393 of the Spanish Ministry for Science and Innovatión.

J.A. Domínguez Pérez, J.M. Muñoz Porras and G. Serrano Sotelo are in the Department of Mathematics, University of Salamanca, Plaza de la Merced 1-4, 37008 Salamanca, Spain (email: jadoming@usal.es, jmp@usal.es, and laina@usal.es).

whose image subspace is the linear code $\mathcal{C} = \mathcal{I}\mathrm{m}\,\mathcal{G} \subseteq \mathbb{F}_q^n$ of length n, dimension k, and rate k/n. $\mathcal{G}$ is called a generator matrix of the code, and $\mathcal{G}'$ is another generator matrix of the code if there exists an element $B \in GL(k, \mathbb{F}_q)$ such that $\mathcal{G}' = B \cdot \mathcal{G}$.

In practical applications, the codification process is not limited to a single word, but to a sequence of information words depending on time, $u_t \in \mathbb{F}_q^k$, $t \geq 0$, which after the codification are transformed into the sequence of codified words $x_t = u_t\mathcal{G}$ and x_t at the instant t depends only on the information word u_t at the same instant t.

The basic idea of *convolutional codification* is to allow x_t to depend not only on u_t but also on $u_{t-1}, \dots, u_{t-m}$ for some positive integer m, which is the *memory* of the code. If one denotes a sequence of words as a polynomial vector $u(z) = \sum_{t=0} u_t z^t \in \mathbb{F}_q[z]^k$ and the product by z^i as a *delay operator*, $z^i u(z) = \sum_{t=0} u_t z^{t+i} = \sum_{t=i} u_{t-i} z^t$, each $k \times n$ matrix $\mathcal{G}$ of rank k with entries in $\mathbb{F}_q[z]$ defines an injective morphism of $\mathbb{F}_q[z]$-modules

$$\begin{aligned} \mathbb{F}_q[z]^k &\overset{\mathcal{G}}{\to} \mathbb{F}_q[z]^n \\ u(z) &\mapsto x(z) = u(z)\mathcal{G} \end{aligned}$$

and one says that the image submodule is a *convolutional code*, $\mathcal{C} = \mathcal{I}\mathrm{m}\,\mathcal{G} \subseteq \mathbb{F}_q[z]^n$, of length n and dimension k, and that $\mathcal{G}$ is a generator matrix of $\mathcal{C}$. One can then define *a rate k/n convolutional code $\mathcal{C}$ as a submodule of rank k of $\mathbb{F}_q[z]^n$*.

If we allow the possibility of performing *feedback*, then we can reverse the delay and define convolutional codification over the field of fractions, $\mathbb{F}_q(z)$, of $\mathbb{F}_q[z]$.

Definition 1.1. *A rate k/n* convolutional code *$\mathcal{C}$ over $\mathbb{F}_q$ is a $\mathbb{F}_q(z)$-linear subspace of dimension k of $\mathbb{F}_q(z)^n$. The integers (n, k) are called, respectively, the* length *and* dimension *of the convolutional code.*

Each *generator matrix* $\mathcal{G}$ of $\mathcal{C}$ with entries in $\mathbb{F}_q(z)$ defines an injective linear *encoding map*:

$$\begin{aligned} \mathbb{F}_q(z)^k &\overset{\mathcal{G}}{\to} \mathbb{F}_q(z)^n \\ u(z) &\mapsto x(z) = u(z)\mathcal{G}\,, \text{ such that } \mathcal{I}\mathrm{m}\,\mathcal{G} = \mathcal{C}. \end{aligned}$$

Given two generator matrices $\mathcal{G}$ and $\mathcal{G}'$ of the convolutional code $\mathcal{C}$, there exists an element $B \in GL(k, \mathbb{F}_q(z))$ such that $\mathcal{G}' = B \cdot \mathcal{G}$.

If $\mathcal{G}$ and $\mathcal{G}'$ are *polynomial generator matrices* of $\mathcal{C}$, that is, with entries in $\mathbb{F}_q[z]$, then their image submodules, as morphisms of $\mathbb{F}_q[z]$-modules $\mathbb{F}_q[z]^k \xrightarrow{\mathcal{G},\mathcal{G}'} F_q[z]^n$, satisfy

$$\mathcal{I}\mathrm{m}\,\mathcal{G} \otimes_{\mathbb{F}_q[z]} \mathbb{F}_q(z) = \mathcal{C} = \mathcal{I}\mathrm{m}\,\mathcal{G}' \otimes_{\mathbb{F}_q[z]} \mathbb{F}_q(z);$$

although, they may be different: $\mathcal{I}\mathrm{m}\,\mathcal{G} \neq \mathcal{I}\mathrm{m}\,\mathcal{G}'$.

Thus, we are interested in polynomial generator matrices that define the same submodule. The family of the polynomial generator matrices called *basic* ([4], [6]), satisfies this property.

1.1. Basic generator matrices. Degree of a convolutional code.

Let $\mathcal{C} \subseteq \mathbb{F}_q(z)^n$ be a (n, k) convolutional code.

Definition 1.2. *A polynomial generator matrix $\mathcal{G}$ of $\mathcal{C}$, $\mathbb{F}_q[z]^k \xrightarrow{\mathcal{G}} F_q[z]^n$, is basic if any of the following equivalent conditions are satisfied:*

1. *The quotient module $\mathbb{F}_q[z]^n / \mathcal{I}\mathrm{m}\,\mathcal{G}$ is free.*
2. *The invariant factors of $\mathcal{G}$ are all equal to one.*
3. *The greatest common divisor of the order k minors of $\mathcal{G}$ is equal to one.*
4. *$\mathcal{G}$ has a right inverse in $\mathbb{F}_q[z]$.*

The existence of basic matrices for all convolutional codes was proved in a constructive way by Forney [4], using the Smith algorithm for the computation of invariant factors ([3],Theorem 11.16).

Theorem 1.3. ([3]) *Let $\mathbb{F}_q[z]^k \xrightarrow{\mathcal{G},\mathcal{G}'} F_q[z]^n$ be two polynomial generator matrices of $\mathcal{C}$. One has:*

1. *If $\mathcal{G}$ is basic and $\mathcal{I}\mathrm{m}\,\mathcal{G} \subseteq \mathcal{I}\mathrm{m}\,\mathcal{G}'$, then $\mathcal{I}\mathrm{m}\,\mathcal{G} = \mathcal{I}\mathrm{m}\,\mathcal{G}'$.*
2. *If $\mathcal{G}$ and $\mathcal{G}'$ are basic, then $\mathcal{I}\mathrm{m}\,\mathcal{G} = \mathcal{I}\mathrm{m}\,\mathcal{G}'$; that is, basic generator matrices define the same submodule.*

Theorem 1.4. ([3],[6]) *The family of the basic generator matrices is invariant under the action of the unimodular group $GL(k, \mathbb{F}_q[z])$. Thus, the number*

$$\delta_{\mathcal{G}} = \textit{maximum degree of the order } k \textit{ minors of } \mathcal{G}$$

is the same for all basic encoders.

One can now consider an invariant associated with the code, namely, the degree of the code, which is defined as follows:

Definition 1.5. *The degree δ of a convolutional code $\mathcal{C}$ is*

$$\delta = \delta_{\mathcal{G}}\,, \ \textit{where } \mathcal{G} \textit{ is any basic encoder of } \mathcal{C}.$$

1.2. Minimal basic generator matrices. Canonical matrices.

In the implementation of convolutional codes as physical devices it is convenient to find *minimal encoders*, in the sense that the corresponding circuit will have the minimum possible quantity of memory boxes. The formalization of the concept of minimality can be expressed in terms of the degree δ of the code.

If $\mathcal{G}$ is a polynomial generator matrix of $\mathcal{C}$, one denotes by $\deg \mathcal{G}$ the sum of its row degrees.

Theorem 1.6. [4] *For each (n, k) convolutional code of degree δ there exists at least one basic generator matrix $\mathcal{G}$ such that*

$$\delta = \deg \mathcal{G}\,.$$

Moreover,

$$\deg \mathcal{G} \leq \deg \mathcal{G}'$$

for all polynomial encoders $\mathcal{G}'$ of the convolutional code.

These basic generator matrices were called *minimal basic matrices* by Forney [4] or *canonical matrices* by McEliece [6].

1.3. **Dual code. Control matrix.**

Given an (n,k)-convolutional code $\mathcal{C} \subseteq \mathbb{F}_q(z)^n$, the dual code is the $\mathbb{F}_q(z)$-subspace defined by

$$\mathcal{C}^\perp = \{y(z) \in \mathbb{F}_q(z)^n \;/\; \langle x(z), y(z)\rangle = 0 \text{ for every } x(z) \in \mathcal{C}\}\,,$$

with respect to the pairing $\langle x(z), y(z)\rangle = \sum_{i=1}^n x_i(z)y_i(z)$, where $x(z) = (x_1(z), \dots, x_n(z))$ and $y(z) = (y_1(z), \dots, y_n(z))$ are in $\mathbb{F}_q(z)^n$.

Theorem 1.7. *(*[3]*,Theorem 11.28) $\mathcal{C}^\perp$ is an $(k, n-k)$* convolutional code with the same degree as $\mathcal{C}$*.*

One defines a *control matrix* for $\mathcal{C}$ as a $n-k \times n$ generator matrix H of its dual code $\mathcal{C}^\perp$.

1.4. **Weights and Free Distance.**

The *(Hamming) weight* of a vector $x = (x_1, \dots, x_n) \in \mathbb{F}_q^n$ is given by $w(x) = \#\{i \mid x_i \neq 0\}$ and the *(Hamming) distance* between $x, y \in \mathbb{F}_q^n$ is defined as the weight $w(y-x)$.

In the case of convolutional codes, one needs an analogous notion for polynomial vectors $x(z) = (x_1(z), \dots, x_n(z)) \in \mathbb{F}_q[z]^n$. If one writes $x(z) \in \mathbb{F}_q[z]^n$ as a polynomial with vector coefficients,

$$x(z) = \sum_t x_t z^t\,, \text{ where } x_t = (x_{t1}, \dots, x_{tn}) \in \mathbb{F}_q^n\,,$$

then one can define a natural notion of *weight in convolutional coding theory* as folows:

Definition 1.8. *The* weight *of $x(z) \in \mathbb{F}_q[z]^n$ is*

$$w(x(z)) = \sum_t w(x_t)\,.$$

Definition 1.9. *The free distance of an (n,k) convolutional code $\mathcal{C} \subseteq \mathbb{F}_q(z)^n$ is*

$$d_{\mathit{free}} = \min\{w(x(z)) \mid x(z) \in \mathcal{C} \cap \mathbb{F}_q[z]^n\,,\ x(z) \neq 0\}\,.$$

In particular, if the degree of the code is zero, $\mathcal{C}$ is a linear code and the (free) distance is the (minimum) distance as linear code.

One says that a linear code $\mathcal{C}(n,k)$ is MDS if its Hamming distance attains the Singleton bound $n-k+1$. Analogously one has:

Definition 1.10. *A convolutional code is MDS if its free distance d_{free} attains the generalized* Singleton bound [7]*; that is,*

$$d_{\mathit{free}} = (n-k)(\lfloor \delta/k \rfloor + 1) + \delta + 1\,,$$

where n, k and δ are respectively the length, dimension and degree of the convolutional code, $C(n,k,\delta)$.

In order to compute the free distance of a one-dimensional convolutional code $C(n,1,\delta)$ in terms of the polynomial decomposition of a canonical generator matrix

$$\mathcal{G} = G_0 + G_1 z + G_2 z^2 + \dots + G_\delta z^\delta\,,$$

it is usefull to know the Hamming weights of the linear codes G_j, and of the linear codes $\begin{pmatrix} G_j \\ \vdots \\ G_0 \end{pmatrix}$ and $\begin{pmatrix} G_\delta \\ \vdots \\ G_{\delta-j} \end{pmatrix}$, for all $0 \le j \le \delta$.

Theorem 1.11. *If the codes G_j are MDS for all $0 \le j \le \delta$ and the codes $\begin{pmatrix} G_j \\ \vdots \\ G_0 \end{pmatrix}$ and $\begin{pmatrix} G_\delta \\ \vdots \\ G_{\delta-j} \end{pmatrix}$ are $(n, j+1)$ linear codes and MDS for all $0 \le j \le \delta$, then $\delta < n$, $C(n,1,\delta)$ is a MDS convolutional code, and $\mathcal{G} = G_0 + G_1 z + G_2 z^2 + \cdots + G_\delta z^\delta$ is a generator matrix.*

Proof. Note first that since $\begin{pmatrix} G_\delta \\ \vdots \\ G_0 \end{pmatrix}$ has rank $\delta + 1$ and n columns, one has $\delta < n$.

The polynomial codewords of the code $C(n,1,\delta)$ have the form $p_j(z)G$, where $p_j(z) \in \mathbb{F}_q[z]$ is a polynomial of degree j. Thus, $p_j(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_j z^j$, with $a_j \neq 0$. Moreover, since the weight does not change as we multiply by z, we can assume that $a_0 \neq 0$.

The polynomial coefficients of the codeword $p_j(z)\mathcal{G}$ are codewords of the linear codes considered in the statement; thus, a lower bound I_j for the weight $w(p_j(z)\mathcal{G})$ is given by the sum of their minimal distances. One has:

$$\begin{aligned} I_0 &= n(\delta+1) \\ I_j &= 2n + 2(n-1) + 2(n-2) + \cdots + 2(n-j+1) + (n-j)(\delta - j + 1)\,, \\ &\quad \text{for } j \le \delta \\ I_{\delta+i} &= I_\delta + i(n-\delta)\,, \text{ for } i \ge 0\,, \end{aligned}$$

which leads to

$$I_j = (j+1)n + (n-j)\delta\,, \text{ for every } j \ge 0\,.$$

Since $I_{j+1} - I_j = n - \delta > 0$, for $j \ge 0$, the free distance of the code is

$$d_{free}(C(n,1,\delta)) = I_0 = n(\delta+1)\,.$$

Thus, $C(n,1,\delta)$ is a MDS convolutional code. □

Convolutional Goppa codes provide examples of this situation, as we shall see later in this paper.

2. Summary of Convolutional Goppa Codes Theory

Let $(X, \mathcal{O}_X)$ be a smooth projective curve over $\mathbb{F}_q(z)$ of genus g, and let Σ_X be the field of rational functions of X; we also assume that $\mathbb{F}_q(z)$ is algebraically closed in Σ_X.

Given a set $p_1, \ldots, p_n$ of n different $\mathbb{F}_q(z)$-rational points of X, if $\mathcal{O}_{p_i}$ denotes the local ring at the point p_i, with maximal ideal $\mathfrak{m}_{p_i}$, and t_i is a local parameter at p_i, one has the exact sequences

$$\begin{aligned} 0 \to \mathfrak{m}_{p_i} \to \mathcal{O}_{p_i} \to \mathcal{O}_{p_i}/\mathfrak{m}_{p_i} &\simeq \mathbb{F}_q(z) \to 0 \\ s(t_i) &\mapsto s(p_i)\,. \end{aligned} \tag{1}$$

Let us consider the divisor $D = p_1 + \dots + p_n$, with its associated invertible sheaf $\mathcal{O}_X(D)$. One has an exact sequence of sheaves

$$0 \to \mathcal{O}_X(-D) \to \mathcal{O}_X \to Q \to 0\,, \tag{2}$$

where the quotient Q is a sheaf with support at the points p_i.

Let G be a divisor on X of degree r, with support disjoint from D. Tensoring the exact sequence (2) by the associated invertible sheaf $\mathcal{O}_X(G)$, one obtains

$$0 \to \mathcal{O}_X(G-D) \to \mathcal{O}_X(G) \to Q \to 0\,. \tag{3}$$

For each divisor F over X, let us denote their $\mathbb{F}_q(z)$-vector space of global sections by

$$L(F) \equiv \Gamma(X, \mathcal{O}_X(F)) = \{s \in \Sigma_X \mid (s) + F \geq 0\}\,,$$

where (s) is the divisor defined by $s \in \Sigma_X$. Taking global sections in (3), one obtains

$$\begin{aligned} 0 \to L(G-D) \to L(G) \xrightarrow{\alpha} \mathbb{F}_q(z) \times &\overset{n}{\dots} \times \mathbb{F}_q(z) \to \dots \\ s \mapsto (s(p_1), &\dots, s(p_n))\,. \end{aligned}$$

Definition 2.1. ([1],[2]) *The convolutional Goppa code $\mathcal{C}(D,G)$ associated with the pair (D,G) is the image of the $\mathbb{F}_q(z)$-linear map*

$$\alpha\colon L(G) \to \mathbb{F}_q(z)^n$$

Analogously, given a subspace $\Gamma \subseteq L(G)$, one defines the convolutional Goppa code $\mathcal{C}(D,\Gamma)$ as the image of $\alpha_{|\Gamma}$.

By construction, $\mathcal{C}(D,G)$ is a convolutional code of length n and dimension

$$k \equiv \dim L(G) - \dim L(G-D)\,.$$

Under the condition $2g-2 < r < n$, the evaluation map $\alpha\colon L(G) \hookrightarrow \mathbb{F}_q(z)^n$ is injective, and the dimension of $\mathcal{C}(D,G)$ is

$$k = r + 1 - g\,.$$

The dual convolutional Goppa code of the code $\mathcal{C}(D,G)$ is the $\mathbb{F}_q(z)$-linear subspace $\mathcal{C}^\perp(D,G)$ of $\mathbb{F}_q(z)^n$ given as in 1.3.

As we proved in [1, §3], the dual convolutional Goppa code $\mathcal{C}^\perp(D,G)$ associated with the pair (D,G) is the image of the $\mathbb{F}_q(z)$-linear map $\beta\colon L(K+D-G) \to \mathbb{F}_q(z)^n$, given by

$$\beta(\eta) = (\operatorname{Res}_{p_1}(\eta), \dots, \operatorname{Res}_{p_n}(\eta))\,,$$

where K is the canonical divisor of rational differential forms over X.

Since we are taking $2g-2 < r < n$, the map β is injective, and $\mathcal{C}^\perp(D,G)$ is a convolutional code of length n and dimension

$$\dim L(K+D-G) = n - (1 - g + r)\,.$$

2.1. Convolutional Goppa Codes over the projective line.

Let $X = \mathbb{P}^1_{\mathbb{F}_q(z)} = \operatorname{Proj} \mathbb{F}_q(z)[x_0, x_1]$ be the projective line over the field $\mathbb{F}_q(z)$, and let us denote by $t = x_1/x_0$ the affine coordinate, by $p_0 = (1, 0)$ the origin point, and by $p_\infty = (0, 1)$ the point at infinity.

Let us take $p_1, \dots, p_n$ different rational points of $\mathbb{P}^1$ and the divisors

$$\begin{aligned} D &= p_1 + \cdots + p_n \\ G &= rp_\infty - sp_0 \text{ , with } 0 \leq s \leq r < n \end{aligned}$$

Since $g = 0$, the evaluation map $\alpha \colon L(G) \to \mathbb{F}_q(z)^n$ is injective, and $\mathcal{I}\mathrm{m}\, \alpha$ defines a convolutional Goppa code $\mathcal{C}(D, G)$ of length n and dimension $k = r - s + 1$.

If $\alpha_i \in \mathbb{F}_q(z)$, $1 \leq i \leq n$, is the local coordinate of the rational point $p_i \in \mathbb{P}^1_{\mathbb{F}_q(z)}$, so that

$$\alpha_i = a_i z + b_i, \text{ with } a_i \neq 0 \text{ , } b_i \in \mathbb{F}_q,$$

then, the matrix of the evaluation map α with respect to the basis $\{t^s, t^{s+1}, \dots, t^r\}$ of $L(G)$ is the following generator matrix for the code $\mathcal{C}(D, G)$:

$$\mathcal{G} = \begin{pmatrix} \alpha_1^s & \alpha_2^s & \dots & \alpha_n^s \\ \alpha_1^{s+1} & \alpha_2^{s+1} & \dots & \alpha_n^{s+1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^r & \alpha_2^r & \dots & \alpha_n^r \end{pmatrix} . \tag{4}$$

We proved in [1, §5] that the parity-check matrix H, with respect to the basis

$$\left\langle \frac{dt}{t^s \prod_{i=1}^{n} (t - \alpha_i)}, \frac{t\, dt}{t^s \prod_{i=1}^{n} (t - \alpha_i)}, \dots, \frac{t^{n-r+s-2} dt}{t^s \prod_{i=1}^{n} (t - \alpha_i)} \right\rangle \text{ of } L(K + D - G),$$

is:

$$H = \begin{pmatrix} h_1 & h_2 & \dots & h_n \\ h_1 \alpha_1 & h_2 \alpha_2 & \dots & h_n \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ h_1 \alpha_1^{n-r+s-2} & h_2 \alpha_2^{n-r+s-2} & \dots & h_n \alpha_n^{n-r+s-2} \end{pmatrix} , \tag{5}$$

where $h_j = \dfrac{1}{\alpha_j^s \prod\limits_{\substack{i=1 \\ i \neq j}}^{n} (\alpha_j - \alpha_i)}$.

3. One-dimensional Convolutional Goppa Codes over $\mathbb{P}^1_{\mathbb{F}_q(z)}$

We shall construct two families of examples of one dimensional convolutional codes over $\mathbb{P}^1_{\mathbb{F}_q(z)}$ with canonical generator matrices [6], whose free distance, d_{free}, attains the generalized Singleton bound, i.e., they are MDS convolutional codes [7] (Theorems 3.1 and 3.2).

Let $L(G) = \langle t^s, t^{s+1}, \dots, t^r \rangle \xrightarrow{\alpha} \mathbb{F}_q(z)^n$ be the evaluation map associated with the divisors $D = p_1 + \cdots + p_n$ and $G = rp_\infty - sp_0$, $0 \leq s \leq r < n$, as in Section 2.

Let us denote by $CGC(n, 1)$ the one-dimensional convolutional Goppa code defined by restriction of the evaluation map α to the subspace

$$\Gamma = \langle t^s + t^{s+1} + \cdots + t^r \rangle \subseteq L(G) \,.$$

If a_iz+b_i, with $a_i\neq 0$, $b_i\in\mathbb{F}_q$, is the local coordinate of the rational point $p_i\in\mathbb{P}^1_{\mathbb{F}_q(z)}$, a generator matrix for the code $CGC(n,1)$ is

$$\mathcal{G}=\begin{pmatrix}\sum_{i=s}^{r}(a_1z+b_1)^i & \sum_{i=s}^{r}(a_2z+b_2)^i & \dots & \sum_{i=s}^{r}(a_nz+b_n)^i\end{pmatrix}$$

We shall describe particular cases of these codes and we shall prove that some of these codes are MDS convolutional codes.

Theorem 3.1. *If $s=r$, a generator matrix of the code $CGC(n,1)$ is:*

$$\begin{pmatrix}(a_1z+b_1)^r & (a_2z+b_2)^r & \dots & (a_nz+b_n)^r\end{pmatrix}\ .$$

If we choose a_i,b_i for each $1\leq i\leq n$, such that $\frac{b_i}{a_i}=c^{i-1}$, where c is a primitive element of $\mathbb{F}_q$, a generator matrix of the code $CGC(n,1)$ is:

$$\mathcal{G}=\begin{pmatrix}a_1^r(z+1)^r & a_2^r(z+c)^r & a_3^r(z+c^2)^r & \dots & a_n^r(z+c^{n-1})^r\end{pmatrix}\ .$$

The matrix $\mathcal{G}$ is canonical and the code defined by $\mathcal{G}$ is MDS.

Proof. $\mathcal{G}$ is clearly canonical.

The memory and the degree δ of $CGC(n,1)$ are equal to r, so that the generalized Singleton bound is $n(r+1)$.

The polynomial decomposition of $\mathcal{G}$ is

$$\mathcal{G}=G_0+G_1z+G_2z^2+\dots+G_rz^r\ ,\ \text{where}$$
$$G_j=\binom{r}{j}\begin{pmatrix}a_1^r & a_2^rc^{r-j} & a_3^rc^{2(r-j)} & \cdots & a_n^rc^{(n-1)(r-j)}\end{pmatrix}\ ,\ \text{with } j=0,1,\dots,r\,,$$

It is clear that for all $0\leq j\leq r$ the linear codes G_j , $\begin{pmatrix}G_j\\ \vdots\\ G_0\end{pmatrix}$, and $\begin{pmatrix}G_r\\ \vdots\\ G_{r-j}\end{pmatrix}$ are MDS evaluation codes with Hamming distances equal to n, $n-j$, and $n-j$, respectively. Then, as we proved in Theorem 1.11, the convolutional Goppa code $CGC(n,1)$ is MDS. □

Theorem 3.2. *Let us consider the case when $s=0$ (so that $\Gamma=\langle 1+t+t^2+\cdots t^r\rangle$), all b_i's are equal, $b_i=b$, and $a_i=a^{i-1}$ where a is an element of $\mathbb{F}_q$ with* $\operatorname{order}(a)\geq n$. *Then, the generator matrix of the code $CGC(n,1)$*

$$\mathcal{G}=\begin{pmatrix}\sum_{i=0}^{r}(z+b)^i & \sum_{i=0}^{r}(az+b)^i & \dots & \sum_{i=0}^{r}(a^{n-1}z+b)^i\end{pmatrix}\ ,$$

is canonical and the code $CGC(n,1)$ is an MDS convolutional code of degree r and free distance $n(r+1)$.

Proof. If one denotes $c_j=\sum_{m=j}^{r}\binom{m}{j}b^{m-j}$, $0\leq j\leq r$, the polynomial decomposition of $\mathcal{G}$ is

$$\mathcal{G}=G_0+G_1z+G_2z^2+\dots+G_rz^r\ ,\ \text{where}$$
$$G_j=c_j\begin{pmatrix}1 & a^j & a^{2j} & \cdots & a^{(n-1)j}\end{pmatrix}\ ,\ \text{with } j=0,1,\dots,r\,.$$

The linear codes $L_{j,i} = \begin{pmatrix} G_i \\ G_{i-1} \\ \vdots \\ G_{i-j} \end{pmatrix}, 0 \leq j \leq i \leq r$, are also MDS evaluation codes with Hamming distance $d(L_{j,i}) = n - j$, and hence $CGC(n,1)$ is a MDS convolutional Goppa code. □

Remark 3.3. *In the case $b_i = 0$, a generator matrix of the above MDS code is:*

$$\mathcal{G} = \sum_{i=0}^{r} z^i \begin{pmatrix} 1 & a^i & a^{2i} \dots & a^{(n-1)i} \end{pmatrix}$$

and we obtain the class of one dimensional MDS convolutional codes of parameters $(n, 1, r)$ constructed by Gluesing and Langfeld [5].

3.1. Classification of one-dimensional Convolutional Goppa Codes over the projective line.

Each one-dimensional convolutional Goppa code over $\mathbb{P}^1_{\mathbb{F}_q(z)}$ is defined by a subspace Γ of dimension one of the vector space $L(G)$. We can therefore identify the set of one-dimensional convolutional Goppa codes with the projective space $\mathbb{P}(L(G))$ which is a variety of dimension $r - s$ over $\mathbb{F}_q$ since $L(G) = \langle t^s, \dots, t^r \rangle$.

Explicitly, each CGC of dimension one is given by a generator matrix defined by:

$$\Gamma = \langle \lambda_s t^s + \cdots + \lambda_r t^r \rangle \xrightarrow{\mathcal{G}} \mathbb{F}_q(z)^n \, , \, \lambda_i \in \mathbb{F}_q$$

$$\mathcal{G} = \begin{pmatrix} \sum_{i=s}^{r} \lambda_i (a_1 z + b_1)^i & \dots & \sum_{i=s}^{r} \lambda_i (a_n z + b_n)^i \end{pmatrix}$$

Let us consider the case $s = 0$. Here $L(G) = \langle 1, t, \dots, t^r \rangle$ and the set of CGC of dimension one can be identified with the projective space $\mathbb{P}^r_{\mathbb{F}_q}$ of dimension r.

The condition for a code to be MDS is an open condition in $\mathbb{P}^r_{\mathbb{F}_q}$ ([7] Lemma 4.1 and proof Theorem 2.10). Since we have proved in Theorem 3.2 the existence of one dimensional convolutional Goppa codes of the MDS type, the set of MDS Goppa Codes of dimension one is a dense open subset of $\mathbb{P}^r_{\mathbb{F}_q}$ (considering $\mathbb{P}^r_{\mathbb{F}_q}$ as an algebraic variety). Essentially, this means that almost all one-dimensional CGC are of MDS type.

In a forthcoming paper we shall give an explicit characterization of CGC of dimension one that are of MDS type.

References

[1] J. M. Muñoz Porras, J. A. Domínguez Pérez, J. I. Iglesias Curto and G. Serrano Sotelo, "Convolutional codes of Goppa type," *IEEE Trans. Inform. Theory*, vol. 52, pp. 340–344, 2006.

[2] J. A. Domínguez Pérez, J. M. Muñoz Porras, and G. Serrano Sotelo, "Convolutional codes of Goppa type," *Appl. Algebra Engrg. Comm. Comput.*, vol. 15, no. 1, pp. 51–61, 2004.

[3] J. A. Domínguez Pérez, J. M. Muñoz Porras, and G. Serrano Sotelo, *Algebraic geometry constructions of convolutional codes*, in Advances in algebraic geometry codes, pp. 365–391, World Scientific, May 2008.

[4] G.D. Forney Jr, Convolutional codes I: Algebraic structure, *IEEE Trans. Inform. Theory*, **16** (3), 720–738, (1970).

[5] H. Gluesing-Luerssen and B. Langfeld, “A class of one-dimensional MDS convolutional codes,” *Journal of Algebra and its Applications*, vol. 5, pp. 505–520, 2006.

[6] R. J. McEliece, “The algebraic theory of convolutional codes,” in *Handbook of coding theory, Vol. I.* Amsterdam: North-Holland, 1998, pp. 1065–1138.

[7] J. Rosenthal and R. Smarandache, “Maximum distance separable convolutional codes,” *Appl. Algebra Engrg. Comm. Comput.*, vol. 10, no. 1, pp. 15–32, 1999.